TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-interner Workshop

Berlin, 25.06.2026

Prüfung und Zertifizierung von Produkten und Services unter dem CRA

Marcus Sean Geiger, TÜV SÜD

Übersicht CRA

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Produkte mit digitalen Elementen
Jedes Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen

direkte oder indirekte Datenverbindung mit einem Gerät oder Netz

Logische oder physische Datenverbindung

Wenn Ihr Produkt…

- die Kriterien auf der linken Seit erfüllt
- nach 11. Dezember 2027 auf dem EU-Markt in Verkehr gebracht ODER substanziell geändert (Artikel 69) wird
- nicht explizit ausgeschlossen ist (siehe unten)
- keine freie Open-Source-Software (FOSS) ohne Kommerzialisierungsabsicht ist

… gilt der CRA*.

* Ausgenutzte Schwachstellen müssen ab 09/2026 auch für Produkte gemeldet werden, die vor dem CRA in Verkehr gebracht wurden.

Out of Scope

- EU 2018/1139 Civil Aviation
- EU 2017/745 MDR EU 2017/746 IVD
- EU 2019/2144 Motor vehicles
- Verteidigung / Nationale Sicherheit
- 2014/90/EU Schiffsausrüstung
- SaaS (*außer zum Produkt zugehörige "Datenfernverarbeitung slösungen"*)

Anforderungen des CRA

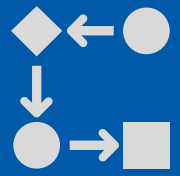
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Berücksichtigung von Cybersicherheit über den **gesamten Produktlebenszyklus**

Meldung aktiv ausgenutzter **Schwachstellen** und von **Vorfällen**

Einhaltung grundlegender **Security-Anforderungen** in den Produkten

Schwachstellenmanagement und kostenlose Security-Updates



Bewertung und Dokumentation von **Cybersicherheitsrisiken**

Klare und verständliche **Bedienungsanleitungen**

CRA Timeline

Regulatorische Fristen

CEN/CENELEC/ETSI Work Programme (M/606)

Beispiele aus den Produktkategorien

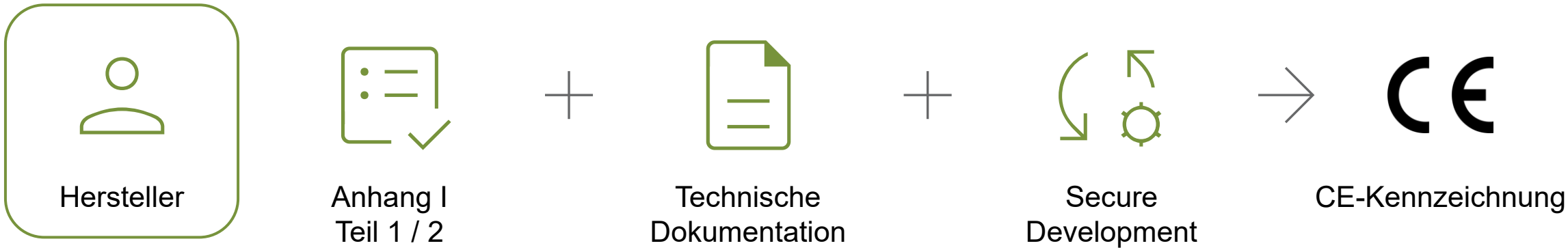
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Standard	Klasse I	Klasse II	Kritisch
▪ Smartphone ▪ Laptop ▪ Videokamera ▪ Steuersoftware ▪ Kopfhörer ▪ …	▪ Identitätsmanagementsysteme ▪ Browser ▪ Passwort-Manager ▪ Anti-Malware-SW ▪ VPN ▪ Netzmanagement-systeme ▪ SIEM ▪ Bootmanager ▪ PKI + SW für digitale Zertifikate ▪ Netzschnittstellen ▪ Betriebssysteme ▪ Router, Modems und Switches ▪ Mikroprozessoren inkl. Security ▪ Mikrocontroller inkl. Security ▪ ASICs und FPGAs inkl. Security ▪ Virtuelle Assistenten ▪ Smart Home inkl. Security ▪ Spielzeug m. Internetanbindung ▪ Health Wearables ex. MDR	▪ Hypervisoren und Container-Runtime-Systeme ▪ Firewalls, IDS, IPS ▪ Manipulationssichere Mikroprozessoren ▪ Manipulationssichere Mikrocontroller	▪ Hardwaregeräte mit Sicherheitsboxen ▪ Smart-Meter-Gateways ▪ Chipkarten, Secure Elements

Konformitätsbewertungsverfahren Modul A

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

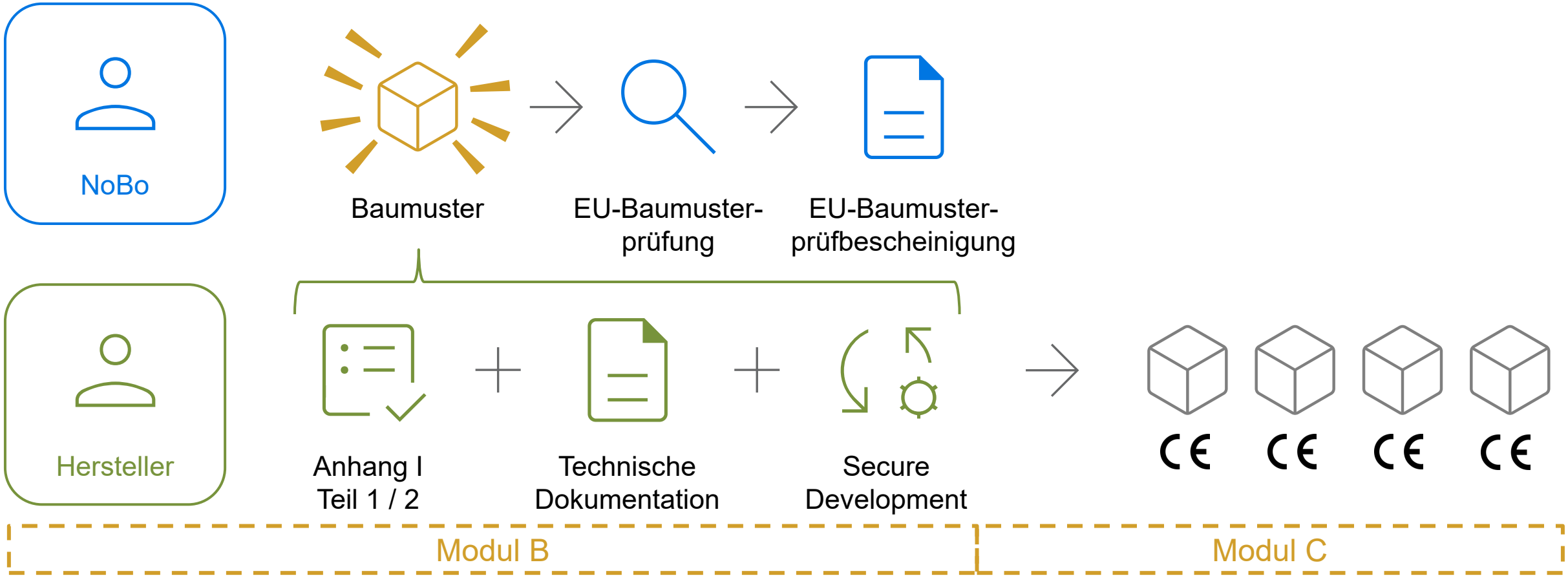
Interne Fertigungskontrolle mit eigenverantwortlicher CE-Kennzeichnung durch den Hersteller



Konformitätsbewertungsverfahren Modul B + C

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

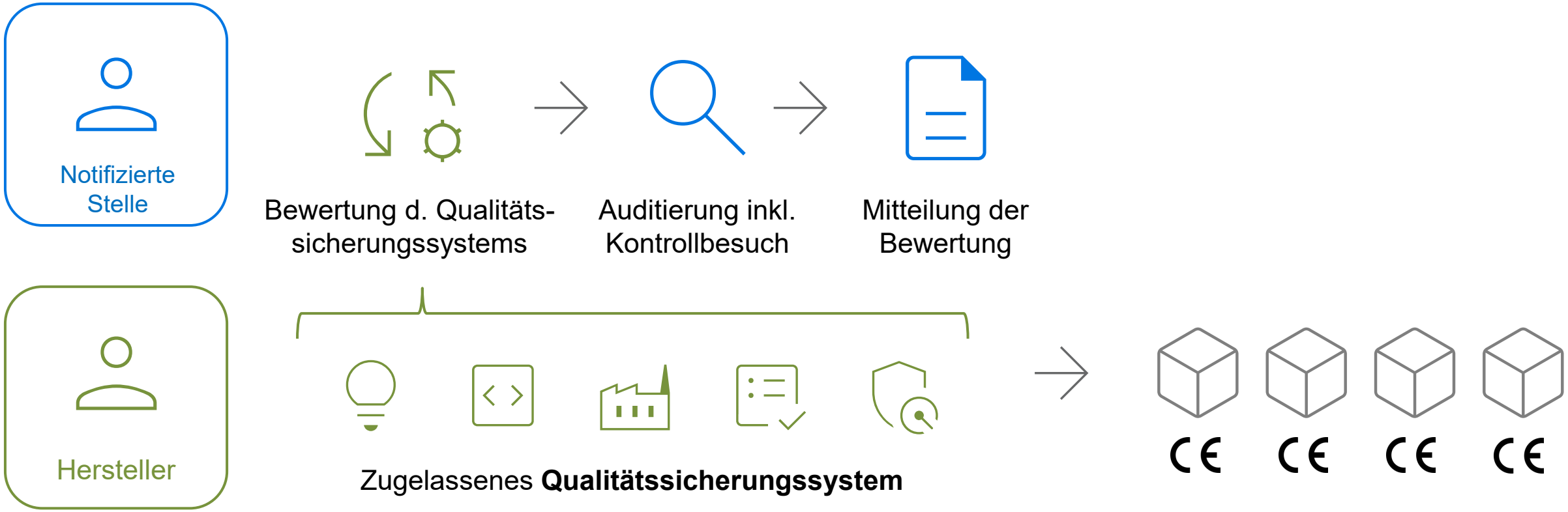
EU-Baumusterprüfung durch notifizierte Stelle und **interne Fertigungskontrolle** mit eigenverantwortlicher CE-Kennzeichnung durch den Hersteller



Konformitätsbewertungsverfahren Modul H

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Umfassende Qualitätssicherung mit Prüfung des Qualitätssicherungssystems durch notifizierte Stelle, CE-Kennzeichnung durch den Hersteller unter Angabe der Kennnummer der notifizierten Stelle



Konformitätsbewertungsverfahren EUCC

Definition & Status

- EUCC ist das erste **europäische System für die Cybersicherheitszertifizierung**, das im Rahmen des **EU-Cybersecurity Act** (Verordnung (EU) 2019/881) angenommen wurde
- Festgelegt durch **Verordnung (EU) 2024/482** (Jan. 2024); Ausstellung von Zertifikaten seit **Feb. 2025**

Freiwilliges System für IKT-Produkte - Hardware, Software, Komponenten (Chips, Chipkarten)

- Beruht auf **ISO/IEC 15408:2022 (CC:2022)** und **ISO/IEC 18045**
- **Nachfolger des SOG-IS MRA** - übernimmt CC-Verfahren; nationale CC-Systeme werden eingestellt

Governance

- **ENISA** - Eigentümer des Systems; pflegt Sachstandsdokumente und Leitlinien
- **NCCAs** (nationale Behörden für die Cybersicherheitszertifizierung) - beaufsichtigen das System; stellen Zertifikate der Stufe 'hoch' aus
- **CABs / ITSEFs** - akkreditierte Konformitätsbewertungsstellen und Prüflabore, die Evaluierungen durchführen

Vertrauenswürdigkeitsstufen *(AVA_VAN-basiert, EAL informativ)*

- **Mittel** - AVA_VAN.1-2 (≈ EAL1-EAL3); Zertifikat von der CAB ausgestellt
- **Hoch** - AVA_VAN.3-5 (≈ EAL4-EAL7); Zertifikat unter Aufsicht der NCCA ausgestellt, mit gegenseitiger Beurteilung (Peer Assessment)
- Stufen oberhalb von AVA_VAN.3 erfordern einen anerkannten **technischen Bereich** oder ein **zertifiziertes PP**

Wesentliche Unterschiede zu klassischen Common Criteria:

- Verpflichtende **Behandlung und Offenlegung von Schwachstellen** über den gesamten Produktlebenszyklus
- Neue **Patch-Management**-Vertrauenswürdigkeitsfamilie (AVA_PAM)
- **Einheitliches EU-weites Zertifikat** + EU-Kennzeichen mit QR-Code
- Weg zur **Konformitätsvermutung mit der Cyberresilienz-Verordnung** (CRA) – (nach Verabschiedung des delegierten Rechtsakts)

Roadmap

- Verordnung **2024/3144** - Übergang zu CC:2022 (CC 3.1r5 nutzbar bis 31. Dez. 2027)
- 2. Änderung (Dez. 2025) - Serienzertifizierung, Aufrechterhaltung der Vertrauenswürdigkeit, Sachstandsdokumente (SotAs)

Produktkategorien und Konformitätsbewertung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Zulässige Konformitätsbewertungsverfahren

Kategorie	Modul A	Modul B + C	Modul H	EUCC
Standard	✓	✓	✓	✓
Klasse 1	⚠ Setzt hEN voraus	✓	✓	✓ mind. substantial
Klasse 2	✗	✓	✓	✓ mind. substantial
Kritisch	✗	✗	✗	✓ mind. substantial

Diskussion: Konformitätsbewertungsverfahren

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Gibt es in dieser Runde ein Interesse, um eine gemeinsame Basis für die Durchführung der Konformitätsbewertungsverfahren nach Modul A “Interne Fertigungskontrolle” zu schaffen?